Appeal No. 2013-1682

United States Court of Appeals for the Federal Circuit

FINJAN INC., a Delaware corporation,

Plaintiff-Appellant,

v.

SYMANTEC CORP., a Delaware corporation, WEBSENSE INC., a Delaware corporation, SOPHOS INC., a Massachusetts corporation,

Defendants-Appellees.

Appeal from the United States District Court for the District of Delaware, Case No. 10-CV-593, Judge Gregory M. Sleet

BRIEF FOR DEFENDANTS-APPELLEES

Jennifer A. Kash
Sean S. Pak
David A. Nelson
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111
Telephone: (415) 875-6600

Attorneys for Defendant-Appellee Symantec Corp.

Anthony M. Stiegler
Lori R. Mason
COOLEY LLP
4401 Eastgate Mall
San Diego, California 92121
Telephone: (858) 550-6000

Attorneys for Defendant-Appellee Websense, Inc.

John Allcock
Sean C. Cunningham
Stanley J. Panikowski
Kathryn Riley Grasso
DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, California 92101
Telephone: (619) 699-2700

Attorneys for Defendant-Appellee Sophos Inc.

CERTIFICATE OF INTEREST

Counsel for Defendant-Appellee, Symantec Corp., certifies the following:

1. The full name of every party represented by us is:

   Symantec Corp.

2. The name of the real party in interest represented by us is:

   Symantec Corp.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

   Symantec Corp. has no parent corporation. There are no publicly held companies that own 10% or more of Symantec's stock.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

   Quinn Emanuel Urquhart & Sullivan LLP by David A. Nelson, Jennifer A. Kash, Sean S. Pak, Mark D. Baker (no longer with the firm), Aaron Perez-Daple (no longer with the firm), Sam Stake, and Howard Chen. Morris, Nichols, Arsht & Tunnel LLP by Jack B. Blumenfeld and Maryellen Noreika.

Dated: February 24, 2014

/s/ Jennifer A. Kash

Jennifer A. Kash
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorney for Defendant-Appellee Symantec Corp.

CERTIFICATE OF INTEREST

Counsel for Defendant-Appellee, Sophos, Inc., certifies the following:

1. The full name of every party represented by us is:

   Sophos, Inc.

2. The name of the real party in interest represented by us is:

   Sophos, Inc.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

   Sophos, Inc. is a wholly owned subsidiary of Sophos Limited which is a privately held company in the United Kingdom. No publicly held corporation directly or indirectly owns 10% or more of its stock.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

   DLA Piper LLP (US) by John Allcock, Sean C. Cunningham, Stanley J. Panikowski, Kathryn Riley Grasso, Brian A. Biggs, Ryan W. Cobb, John Kinton (no longer with the firm), Denise S. Kraft, Megan E. McCarthy (no longer with the firm), Ann A. Parmely (no longer with the firm), Aleine Porterfield (no longer with the firm) and Melissa Puckett (no longer with the firm); and Morris James LLP by Kenneth Laurence Dorsney; and McAndrews IP by Larry Jarvis, George McAndrews and Robert B. Polit.

Dated: February 24, 2014

/s/ John Allcock

John Allcock
DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, California 92101
Telephone: (619) 699-2700

Attorney for Defendant-Appellee Sophos Inc.

CERTIFICATE OF INTEREST

Counsel for Defendant-Appellee, Websense, Inc., certifies the following:

1. The full name of every party represented by us is:

   Websense, Inc.

2. The name of the real party in interest represented by us is:

   N/A

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

   Websense, Inc. is a wholly owned subsidiary of Vista Equity Partners.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

   Anthony M. Stiegler, Paul Batcher, Brian Lam, Jose Rodriguez, and Erin Goodsell of Cooley LLP and John Kyle formerly of Cooley LLP and Thomas Grimm of Morris Nichols Arsht & Tunnell appeared in the district court. Anthony M. Stiegler and Lori R. Mason of Cooley LLP will appear for Websense, Inc. in this Court.

Dated: February 24, 2014

/s/ Anthony M. Stiegler

Anthony M. Stiegler
COOLEY LLP
4401 Eastgate Mall
San Diego, California 92121
Telephone: (858) 550-6000

Attorney for Defendant-Appellee Websense, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Rules

STATEMENT OF RELATED CASES

No other appeal in or from this action has previously been before this or any other appellate court. Finjan and Websense, Inc. are parties to *Finjan, Inc. v. Websense, Inc.*, 3:13-cv-04398 (N.D. Cal. Sept. 23, 2013). There are no other pending cases between the parties to this appeal.

STATEMENT OF THE ISSUES

The issue presented in this appeal is whether the district court correctly upheld the jury's verdict that U.S. Patent Nos. 6,092,194 (the "'194 patent") and 6,480,962 (the "'962 patent") are invalid. More specifically:

1. Was the district court correct in denying Finjan's motions for judgment as a matter of law ("JMOL") that the asserted patents are not invalid where Defendants submitted substantial evidence that the asserted prior art invalidated all of the asserted claims?

2. Was the district court correct in applying its broad discretion to deny Finjan's motion for a new trial?

COUNTER STATEMENT OF THE CASE

In July 2010, Finjan, Inc. ("Finjan") filed a patent-infringement complaint in the District of Delaware against Symantec Corp. ("Symantec"), Websense, Inc. ("Websense"), and Sophos, Inc. ("Sophos") (collectively, "Defendants"). JA311-372. Finjan asserted that Symantec and Sophos infringe the '194 patent and the '962 patent and that Websense infringes the '194 patent. *Id.* The patents relate generally to computer networks and systems and methods for protecting computers and networks from hostile software. JA283, 1:24-27; JA303, 1:21-23. Defendants asserted that neither patent was infringed and that multiple pieces of prior art anticipated and/or rendered obvious the asserted claims of each patent.

On December 21, 2012, after a 13-day trial, the jury returned a verdict of noninfringement and invalidity of all asserted claims. JA3-10. Accordingly, the district court entered judgment in favor of Defendants. JA1-2. Finjan subsequently filed post-trial motions for a new trial and judgment as a matter of law, which the district court denied. JA110. This appeal followed.

INTRODUCTION

The law and substantial evidence support the jury's verdict that the asserted claims of the '194 and '962 patents are invalid, and Finjan has shown no reason to disturb it. Finjan did not appeal the jury's finding that Defendants did not infringe any of the asserted patents, hence waiving any challenge to the noninfringement verdicts. *See* Br., 1-2.

Finjan's disparate objections to the invalidity verdict boil down to: (a) the same attorney argument the jury properly disregarded at trial, (b) citations to testimony from Finjan's experts, which the jury was entitled to discredit, and (c) outright mischaracterizations of the evidence and the law. Having weighed the evidence, including the credibility of the witnesses at trial, the jury correctly returned a verdict of invalidity and noninfringement. Finjan provides no legitimate reason to reverse or vacate that verdict.

COUNTER STATEMENT OF FACTS

I. THE PARTIES.

A. Defendants.

1. Symantec.

Symantec is a global leader in computer security, storage, and systems management products and services. Symantec offers its products and services to businesses and consumers to help them manage their digital information and identities, and it currently employs approximately 20,000 people in over 50 countries. Symantec has invested hundreds of millions of dollars in research and development over the past decade alone and owns more than 1,200 domestic and foreign patents. Its computer and network security solutions offer protection against viruses and malware at numerous points in the network and have been a trusted source of protection for consumers and businesses alike for well over 20 years.

2. Websense.

Websense is a global provider of unified Web, email, mobile and data security solutions designed to protect an organization's data and users from external and internal threats, including modern cyber-threats, advanced malware attacks, information leaks, legal liability and productivity loss. Websense's products and services are sold worldwide to provide content security to enterprise customers, small and medium sized businesses, public sector entities, and Internet

service providers through a network of distributors, value-added resellers and original equipment manufacturers. Websense currently has over 1,500 employees and has offices and operations in San Diego and Los Gatos, California; Reading, England; Beijing, China, and Ra'anana, Israel.

3. Sophos.

Sophos offers award-winning encryption, endpoint security, web, email, mobile and network security backed by SophosLabs, a network of threat intelligence centers. Sophos's products help secure the networks used by 100 million people in 150 countries and 100,000 businesses.

B. Finjan.

Finjan, the owner of the two patents at issue, is a non-practicing entity. It does not manufacture or sell any products, has no ongoing business operations, and has no employees. JA7045, 568:16-569:5; JA7069, 667:2-11; JA7070, 668:4-9. Instead, Finjan is a patent-holding company. JA7770, 668:4-9. In 2009, Finjan sold all of its operations, assets, and product lines to a company called M86 Security ("M86"). JA7053, 600:3-5. Finjan retained ownership in its patent portfolio while M86 took over Finjan's operations. JA7069, 666:22-667:11; JA7070, 668:4-9.

II. THE ASSERTED PATENTS.

The '194 and '962 patents are directed to computer-based systems and methods for preventing harm by malicious "Downloadables." As construed by the district court, a Downloadable is "an executable application program, which is downloaded from a source computer and run on the destination computer." JA1834. The '194 patent describes protecting against malicious Downloadables at the gateway, whereas the '962 patent discloses protection at client computers, *i.e.*, a user's workstation. JA7993, 2083:3-19. A gateway server is used to control communication between client computers (*e.g.*, an internal business network) and terminals or "nodes" on external networks, such as other servers on the Internet. *See* JA14689-709; JA14831-32.

According to Finjan, the asserted patents provided for a new method of virus detection at the gateway server and client computers. While traditional security systems identified threats by looking for known segments of malicious code (*i.e.*, signature scanning), Finjan argues the '194 and '962 patents disclosed a new, proactive detection of malware based on behavior analysis, *i.e.*, based on what the code was going to do as opposed to what the program was. Br., 10-14. But inspecting threats for suspicious behaviors and thereby detecting unknown viruses was well known in the antivirus community before the conception of Finjan's claimed inventions.

A. The '194 Patent.

The '194 patent issued on July 18, 2000 and is entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables." JA271-93. The '194 patent claims priority to Provisional Application No. 60/030,639, filed on November 8, 1996. *Id.* The '194 patent is directed to a form of static analysis performed at a gateway server to protect an internal computer network from suspicious Downloadables. JA283, 1:60-61. As described in the claims, the gateway server receives an incoming Downloadable and compares "a list a [sic] suspicious computer operations that may be attempted by the Downloadable against a security policy to determine if the security policy has been violated." JA287, 10:11-16. If the security policy is violated, execution of the Downloadable is prevented. JA287, 10:16-18.

At trial, Finjan asserted the following claims of the '194 patent against Defendants: 1, 2, 32, 35-37, 58, 65, and 66. JA9057-58. Representative claim 1 is set forth below:

> 1. A computer-based method, comprising the steps of:
> receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;
> comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and
> preventing execution of the Downloadable by the client if the security policy has been violated.

JA287.

B. The '962 Patent.

The '962 patent is entitled "System and Method for Protecting a Client During Runtime from Hostile Downloadables." The '962 patent issued on November 12, 2002. JA294-310. The '962 patent is a continuation of Application No. 08/790,097, filed on January 29, 1997, which claims priority to Provisional Application No. 60/030,639, filed on November 8, 1996. *Id.*

The '962 patent is directed to monitoring multiple subsystems of the operating system of a client computer to protect against malicious Downloadables. JA303, 1:22-24. When an event caused by a request from a Downloadable is detected, the processing of the request is interrupted while information pertaining to the Downloadable is compared against a pre-determined security policy. JA303, 2:25-31. Based on this comparison, the system performs a pre-determined responsive action. *Id.*

At trial, Finjan asserted the following claims of the '962 patent against Symantec: 1, 5, 6, 12, 15, 33, 37, 38, 45, 52, and 55. JA9057. With respect to Sophos, Finjan asserted claims 1, 5, 6, 12, 21, 33, 37, 38, 45, and 52. *Id.* Representative claim 1 is set forth below:

> 1. A computer-based method, comprising:
> monitoring substantially in parallel a plurality of subsystems of the operating

system during runtime for an event caused from a request made by a Downloadable;
interrupting processing of the request;
comparing information pertaining to the Downloadable against a predetermined security policy; and
performing a predetermined responsive action based on the comparison.

JA306.

III. EXPERTS.

At trial, Defendants presented two invalidity experts, Dr. Eugene Spafford and Mr. David Klausner. In rebuttal, Finjan presented its invalidity rebuttal expert, Dr. Giovanni Vigna.

A. Dr. Eugene Spafford.

Dr. Spafford has over 30 years of experience in the field of computing and computer science, including over 20 years of research and practice in the area of computer security. JA7991, 2075:19-25. His four degrees include a Ph.D. in Computer Science from the Georgia Institute of Technology. JA7990, 2072:23-2073:12. Dr. Spafford is currently a full professor of Computer Science at Purdue University, where he has been employed since 1987. JA7990, 2073:18-23; JA7991, 2074:13-2075:11. He is also the founder and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS), the nation's oldest and largest multidisciplinary academic research institute in information security issues. JA7990, 2073:18-23; JA7991, 2074:3-12.

In addition to his academic experience, Dr. Spafford has served in an advisory or consulting capacity with several U.S. government agencies and their contractors, including the FBI, the U.S. Air Force, and the U.S. Naval Academy. JA7992, 2078:21-2079:15. Dr. Spafford also served on the President's Information Technology Advisory Committee during the Clinton, Bush, and Obama administrations. JA7992, 2079:16-2080:8.

B. David Klausner.

Mr. Klausner holds a bachelor's degree in Mathematics and a Master of Science degree in Electrical Engineering. JA8115, 2403:14-22. He has over 44 years of software development and consulting experience in the computer and software industry as a software developer, manager, company executive, and forensic investigator. JA8115-16, 2404:3-2409:11. Mr. Klausner has spent significant time working with anti-virus software, networks, and network devices such as routers and switches. *Id.*

C. Dr. Giovanni Vigna.

Dr. Vigna is a Professor in the Department of Computer Science at the University of California, Santa Barbara. JA6967, 418:14-21. Dr. Vigna also co-founded and serves as the Chief Technology Officer for Lastline, a company which—like Defendants—develops security products to protect organizations and enterprises from malware. JA6976, 455:11-16. Internal business development

documents reveal that Lastline perceives antivirus security vendors, including Defendant Symantec, as competitors. JA17157; JA6977, 456:14-457:4.

Dr. Vigna chose not to sign the Protective Order. Br., 56; JA8888, 3143:19-3144:10. As a result, Dr. Vigna could not review the source code—which Dr. Medvidovic, Finjan's technical infringement expert, described as "the DNA of the system in question." *Id.*; JA7197, 724:21-725:7. All other experts in the case (including Dr. Medvidovic) relied upon the source code of the relevant products to understand and confirm the functionality of both the accused and prior art products. *Id.*; *see, e.g.*, JA7996, 2097:12-20; JA7998, 2102:3-2105:3; JA8004, 2128:22-2129:3; JA8004-05, 2129:16-2130:13.

IV. THE PRIOR ART.

A. State of the Prior Art.

Computer viruses became more prevalent in the late 1980s and early 1990s because of expanding computer connectivity and growth of data traffic. *See* JA7991, 2077:7-25; JA15244-45. An active antivirus industry and a vibrant community formed to combat this threat and to protect computer systems from attack. The industry began developing software products to detect and remove viruses before they could cause harm, protecting both individual computers and complex networks used by businesses. *See, e.g.*, JA7624, 1822:8-1823:6. By at least 1996, antivirus products were quite sophisticated and included multiple layers

of protection. Following a concept called defense-in-depth, antivirus vendors bundled multiple products together for enterprise customers to include antivirus protection at both the gateway level and on individual client computers within the network to provide multiple lines of defense against malicious software.

1. Static Analysis.

Static analysis refers to examining computer code without running the questionable files. JA7995, 2092:21-2093:5. This analysis is relatively fast and safe because the questionable files are not executed during the analysis. *Id*.

(a) Signature Scanning.

One form of static analysis is traditional signature scanning. Signature scanners were an early tool developed by the antivirus industry to detect viruses. A signature scanner functions by comparing code being scanned against known virus signatures (which are like virus fingerprints) to determine if any of the signatures match. JA7996, 2094:4-15; JA15270; JA16113. If the same pattern exists in the same file being scanned, there is a match, and the system can respond in several ways, including notifying the user of the presence of a virus. *See id.*

As noted, one benefit of traditional signature scanners is that there is no danger of unintentionally harming the computer during the scan, because the code is not executing on the machine during scanning. However, traditional signature scanners were largely limited to the detection of known viruses. JA16113.

(b) Heuristic Scanning.

By the mid-1990s, new viruses were being released frequently, and it required significant effort to develop and release signatures for every new threat in time to be effective. Antivirus researchers recognized the need to provide proactive security against new threats that did not yet have unique signatures identified. *See* JA7996, 2094:16-2095:25; JA15270. Heuristic scanning became a well-known solution to this problem.

In September 1995, the Virus Bulletin Conference published an article regarding heuristic analysis. JA14740-48; JA7996, 2095:6-25. As described in the publication, heuristic analysis provides a mechanism for detecting previously unknown viruses. JA7996, 2095:13-23; JA14745-47. The heuristic scanner can target and detect a group of viruses sharing similar behaviors or operations, regardless of whether the particular virus has been seen before. JA7996, 2094:16-20; JA14745-47. Thus, heuristic analysis could be used to identify previously unknown viruses based on the suspicious behaviors that the program may perform. *Id.*; JA16113. This type of virus protection was available in a variety of commercial products, including ThunderByte, in the mid-1990s.

2. Dynamic Analysis.

Another technique well-known by at least the mid-1990s was dynamic monitoring for virus-like behaviors. JA7996, 2096:1-4. Unlike static scanning,

dynamic monitors operate in real-time while a program is running. JA7996, 2096:5-21. Dynamic monitors add another layer of protection because they can intercept and block unknown viruses based on behavior, such as harmful requests from unknown or unauthorized files. *Id.*; JA15268. This technique of monitoring and intercepting system operations to look for virus-like activities became known as behavior blocking. JA16114-15.

There are several different generations of behavior-blocking systems. First-generation behavior blockers were policy-based. JA16115. Policy-based systems "allow the administrator to specify an explicit blocking policy stating which behaviors are allowed and which are blocked." *Id.* In other words, policy-based behavior blockers use rules to determine how to respond when specific behaviors are detected. JA7627, 1835:25-1837:4; JA16115-16. Policy-based behavior blocking was well-known by 1996. Indeed, Carey Nachenberg, a Fellow and Vice President of Symantec, wrote a policy-based behavior blocker antivirus program in the early 1990s. JA7624, 1822:8-1823:6. Security companies began incorporating policy-based behavior blockers into their antivirus products by at least August 1995. *See* Section IV.C.4 (NAV95).

3. Defense-in-Depth.

"Defense-in-depth" is a well-known principle of security practiced at least since the 1980s. JA7995, 2091:9-24. Defense-in-depth combines multiple security

measures, like the ones described above, to provide a stronger defense than any single measure alone. JA7995, 2091:9-19; JA7630, 1848:14-1849:2. Antivirus products, for example, often come bundled with multiple methods of virus protection. *See* JA7630, 1848:14-1849:2. Defense-in-depth also provides multiple layers of protection within a network by checking for viruses at the gateway server node and again at the client node. *See* JA7995, 2092:7-20.

B. Person of Ordinary Skill in the Art.

Dr. Spafford opined that a person of ordinary skill in the art for the asserted patents in 1996 or early 1997 would hold a bachelor's degree or the equivalent in computer science (or related academic fields) and three to four years of additional experience in the field of computer security or equivalent work experience. JA7995, 2090:17-2091-3. Dr. Spafford based this opinion on his over 25 years of experience in researching, developing, and evaluating computer programs, systems, and architectures, including extensive work related to computer viruses. JA 7995, 2090:5-16.

C. Prior Art References.

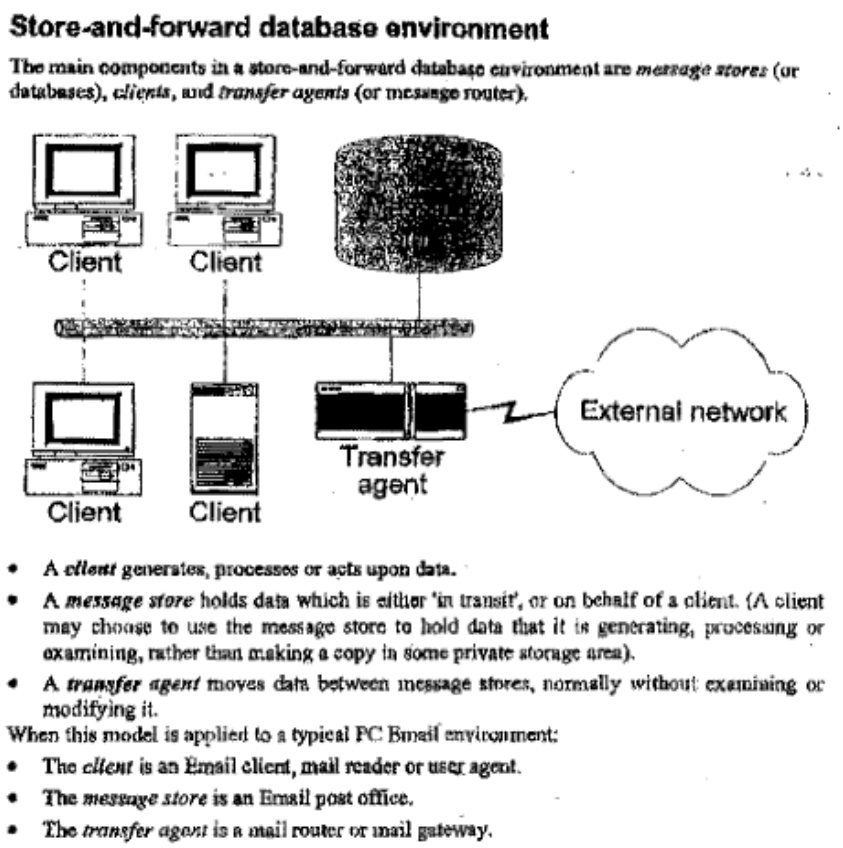
With respect to the '194 patent, Dr. Spafford testified that a combination of MIMEsweeper with ThunderByte 7.0 disclosed all of the elements of the asserted claims. JA8007-08, 2141:24-2143:17. Mr. Klausner testified that Sophos's

SWEEP-InterCheck product disclosed all of the elements of the asserted claims of the ’194 patent. JA8118, 2414:2-7.

As to the ’962 patent, Defendants’ experts testified that SWEEP-InterCheck and the combination of NAV95 and HotJava invalidated the asserted claims. JA7993, 2083:20-2084:6; JA8118, 2414:2-7.

1. MIMEsweeper.

As described above, defense-in-depth provided multiple layers of protection, including protection at the gateway. MIMEsweeper, a software package released in September 1995, used defense-in-depth. JA7994, 2089:6-8; JA14752. As detailed in the *MIMEsweeper Administrator Guide*, dated September 1995, MIMEsweeper described a server that acted as a gateway and included interfaces for software that scanned incoming email messages and files for viruses. JA14752, JA14825. For example:



JA14825. As shown, the transfer agent was an email gateway.

The *Administrator Guide* specified that MIMEsweeper "facilitate[d] the implementation of various functionality and applications at the important Email gateway to external or internal networks." JA14755. MIMEsweeper prevented execution of email attachments that violated a security policy by quarantining the messages at the gateway. JA14831. The *Administrator Guide* further explained that the intended placement of MIMEsweeper was at the gateway server to provide an email gateway for virus scanning. JA8009, 2146:23-2147:24; *see also* JA14831.

Additionally, the MIMEsweeper product described an intention to combine the email gateway software with existing virus scanners, including ThunderByte, to actually analyze incoming e-mail attachments for the presence of malicious software. For example, an M2 Presswire publication from June 1995 explained that "MIMEsweeper has built-in interfaces for the majority of virus protection packages, including ThunderBYTE, F-Prot, Dr Solomon's and Sophos." JA14831; JA8008, 2142:23-2143:8. A Computer Business Review publication similarly noted, "[MIMEsweeper] comes with interfaces for virus protection packages such as Dr. Solomon's, ThunderByte, and F-Prot . . . ." JA14749; *see also* JA14780 ("Any popular virus scanning package can be used, but MIMEsweeper is distributed with a time limited evaluation copy of F-PROT . . . ."). Thus, the press releases and the *Administrator Guide* expressly contemplated that users would combine MIMEsweeper with the ThunderBYTE antivirus software to scan e-mail attachments at the gateway for viruses.

2. ThunderBYTE.

ThunderByte 7.0 was an antivirus program released in the United States (and globally) in February 1996. JA8008, 2144:9-24; JA7994, 2089:9-12; JA16988-90; *see also* JA8008-09, 2145:5- 2146:19; JA17990. The ThunderByte User Manual described a type of heuristic analysis that "detect[ed] yet unknown viruses" by disassembling a file "to detect suspicious instruction sequences." JA15597;

JA8009, 2149:16-2150:2. This analysis was performed by a component, TbScan, that "ha[d] a built-in disassembler and code analyzer." JA15597. Unlike traditional signature scanners, TbScan did not rely on a signature to detect a virus and instead "search[ed] for suspicious instruction sequences" in the executable file being scanned. *Id.*

The User Manual also detailed how ThunderByte detected instructions whose "purpose appears to be formatting a disk, or infecting a file" and then issued a warning. JA15750. If TbScan found a virus, it presented an "action menu," allowing the user to specify actions that prevented "execution of infected programs." JA15607. Finally, the User Manual described how ThunderByte created a substitute non-hostile Downloadable from an infected file. *See* JA15598 (describing how TbClean "disassembles and emulates the infected file and uses this analysis to reconstruct the original file").

3. SWEEP-InterCheck.

SWEEP-InterCheck was developed and sold by Sophos in the early 1990s. During trial, Sophos relied on SWEEP version 2.72 and InterCheck version 2.11, which were sold as a single product in 1994, to prove anticipation of the asserted claims. JA8180-81, 2487:16-2488:1, 2489:22-2490:10; JA8097, 2332:16-18. The SWEEP-InterCheck product detected suspicious computer operations and malware on the computer. JA8096-97, 2327:16-2330:16; JA8097, 2331:6-21, 2332:16-18.

In particular, InterCheck intercepted changed or unknown programs and copied the programs to the server where SWEEP resides. JA8098, 2334:15-2335:16; JA8119, 2418:10-2419:1. SWEEP would then examine the executable and determine whether the program met the appropriate trustworthiness requirements to permit it to run on the computer. *Id*.; JA8098, 2335:17-20.

4. NAV95.

NAV95 was a software program developed and sold by Symantec for use on computers running the Windows 95 operating system. NAV95 was publicly on sale in the United States in August 1995. JA7626-27, 1833:16-1834:1; JA7640, 1888:10-1889:8. NAV95 was designed to protect computers from viruses and other types of malicious code, including unknown viruses. *See* JA17187-88 ("Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform when replicating or attempting to damage files.").

As described in the User Guide, NAV95 included an Auto-Protect feature that monitored subsystems of the operating system for virus-like activity during runtime, allowing it to detect previously unknown viruses based on actions the software programs attempted to execute. JA17271; JA7997, 2098:10-2099:1. In particular, a user of NAV95 was able to configure the software to enforce a

security policy to prevent certain virus-like activities from being performed by a running program. JA17271.

The activities that may have been blocked included low-level format of hard disks, write to hard disk boot records, write to program files, and DOS read-only attribute changes. JA17272. To detect these activities, NAV95 monitored a plurality of subsystems of the operating system, including the file subsystem and the I/O subsystem of the operating system. JA7997-98, 2100:2-2104:15; JA17272; JA29634 (JA7999, 2106:4-21).

Additionally, NAV95 used a component named "SymEvent" to "hook" into file subsystem interrupts, I/O subsystem interrupts, and Windows API's, thereby introducing mechanisms to monitor and intercept requests sent to various subsystems of the operating system. JA7998-99, 2105:4-2107:8. Auto-Protect was the software component of NAV95 that made decisions about security-related events reported by SymEvent. JA17271-72; JA8000, 2110:15-2111:11; JA29638. When Auto-Protect was informed of an event by SymEvent, it performed an analysis to determine how the corresponding request should be handled. JA8000, 2110:15-2112:18. For example, Auto-Protect compared information about the requesting file (*e.g.*, "Downloadable") itself to determine whether the file was excluded from the particular security rule being applied (*e.g.*, whether the file was excluded from a rule that would prevent it from writing to executable files, so that

it was allowed to perform the otherwise-prevented action). *Id*. Auto-Protect also analyzed other information about the requesting file to determine how to handle the request. *See* JA8000, 2111:16-2112:18. After completing the analysis and applying the security policy, Auto-Protect returned its decision to SymEvent, which responded to the instruction by, for example, blocking or allowing the intercepted request. JA8000, 2112:19-2113:14; JA29640 (JA8000, 2112:19-2113:14).

(a) HotJava.

In the 1990s, it was common to install NAV95 on a computer system with a web browser. JA8006, 2135:4-22, 2136:4-12. Doing so provided protection against "Downloadables" received from the Internet and other networks. *Id.* By November 8, 1996, web browsers and browser plug-ins, such as HotJava, supported Java and other scripting languages. JA8004, 2128:2-21. These browsers and plug-ins included built-in security mechanisms, including the runtime protection of the Java Security Manager. JA8005, 2130:4-23. As Dr. Spafford testified, a person of ordinary skill in the art would have been motivated to combine the security mechanisms of Java, *e.g.*, by installing HotJava on the computer system, with the protections provided by other security software to enhance the overall security of the system and provide different layers of

protection according to the well-known defense-in-depth approach. JA8006, 2135:4-22, 2136:4-12.

SUMMARY OF ARGUMENT

Substantial evidence and the patent laws support the jury's verdict finding the asserted claims of the '194 and '962 patents invalid. The anticipation and obviousness arguments presented by the Defendants detailed the disclosure of each element of every asserted claim in the prior art presented at trial and provide more than ample support for the jury's verdict and the district court's orders denying Finjan's post-trial motions.

In particular, the district court properly denied Finjan's motion for a judgment as a matter of law on invalidity as Defendants had presented substantial evidence supporting the jury's finding of invalidity on all asserted claims. Defendants provided evidence, including testimony from witnesses with firsthand experience with the prior art products, source code, manuals, demonstrations of the actual pieces of prior art and the testimony of their experts, to demonstrate that all elements of the asserted claims were disclosed in the prior art. To challenge this evidence, Finjan is able to point only to the testimony of its own expert. A battle of experts, however, does not give rise to a judgment as a matter of law.

Additionally, the district court properly applied its broad discretion in denying Finjan's motion for a new trial. The district court's preclusion of Finjan's

expert's misleading testimony was proper, and the jury's verdict was not against the weight of the evidence. Further, Finjan waived any appeal regarding alleged inconsistency in the verdict and, in any event, the jury's verdict was not inconsistent.

In the end, Finjan provides no basis to reverse the jury's findings or the district court's rulings on the post-trial motions.

ARGUMENT

I. STANDARD OF REVIEW

This Court reviews a denial of a JMOL *de novo*, "reapplying the district court's JMOL standard anew." *Union Carbide Chems. & Plastics Tech. Corp. v. Shell Oil Co.*, 308 F.3d 1167, 1185 (Fed. Cir. 2002). Finjan "must show that the jury's findings, presumed or express, are not supported by substantial evidence or, if they were, that the legal conclusion(s) implied [by] the jury's verdict cannot in law be supported by those findings." *CNH Am. LLC v. Kinze Mfg.*, 809 F. Supp. 2d. 280, 284 (D. Del. 2011) (citations omitted). "Substantial evidence" is "such relevant evidence from the record taken as a whole as might be accepted by a reasonable mind as adequate to support the finding under review." *Perkin-Elmer Corp. v. Computervision Corp.*, 732 F.2d 888, 893 (Fed. Cir. 1984).

JMOL is appropriate only "if, viewing the evidence in the light most favorable to the nonmovant and giving it the advantage of every fair and

reasonable inference, there is insufficient evidence from which a jury reasonably could find liability." *Lightning Lube, Inc. v. Witco Corp.*, 4 F.3d 1153, 1166 (3d Cir. 1993) (citing *Wittekamp v. Gulf & Western, Inc.*, 991 F.2d 1137, 1141 (3d Cir. 1993)). "In determining whether the evidence is sufficient to sustain liability, the court may not weigh the evidence, determine the credibility of witnesses, or substitute its version of the facts for the jury's version." *Id.* (citing *Fineman v. Armstrong World Indus., Inc.*, 980 F.2d 171, 190 (3d Cir. 1992)). Rather, the court must resolve all conflicts of evidence in the non-movant's favor. *Williamson v. Consol. Rail Corp.*, 926 F.2d 1344, 1348 (3d Cir. 1991). A court should grant JMOL only if "the record is critically deficient of the minimum quantum of evidence. . . ." *Gomez v. Allegheny Health Servs., Inc.*, 71 F.3d 1079, 1083 (3d Cir. 1995).

Regional circuit law governs this Court's standard of review of a district court's ruling on a motion for new trial. *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1361 (Fed.Cir.1999). A district court should grant a new trial on the basis that the jury's verdict is against the weight of the evidence only where "a miscarriage of justice would result if the verdict were to stand." *Fineman*, 980 F.2d at 211 (quoting *Williamson*, 926 F.2d at 1352). In the Third Circuit, a district court's denial of a motion for a new trial is reviewed for an abuse of discretion. *Montgomery County v. Microvote Corp.*, 320 F.3d 440, 445 (3d Cir. 2003).

II. SUBSTANTIAL EVIDENCE SUPPORTS THE JURY'S VERDICT THAT THE ASSERTED CLAIMS ARE INVALID.

A. Defendants Presented Substantial Evidence That the '194 Patent Is Invalid.

Defendants presented substantial evidence that the asserted claims of the '194 patent are invalid in light of ThunderByte, MIMEsweeper, and SWEEP-InterCheck.

1. Defendants Presented Substantial Evidence That the '194 Patent Was Obvious in Light of ThunderByte 7.0 Combined with MIMEsweeper.

(a) Defendants Presented Substantial Evidence That There Was a Reasonable Expectation of Success Combining ThunderByte 7.0 with MIMEsweeper.

To prove obviousness, "only a reasonable expectation of success, not a guarantee, is needed." *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1364 (Fed. Cir. 2007). The evidence showed not only that there was a "reasonable expectation of success" of combining ThunderByte 7.0 with MIMEsweeper, but also that MIMEsweeper was in fact *designed* to be combined with ThunderByte 7.0. JA8008, 2142:5-2143:17; JA8009, 2146:23-2147:6; JA14749-50; JA14825; JA14831-32.

Dr. Spafford used two press releases to prove this point. The first press release stated that MIMEsweeper had "built-in interfaces for the majority of virus protection packages, including ThunderByte." JA8008, 2142:5-2143:8; JA14831-32. Dr. Spafford explained to the jury that the "built-in interfaces" meant "that

[MIMEsweeper] was *designed* already so that you could simply slot in any of the programs that are listed there, ThunderByte, . . . without having to do any signature changes to the software." JA8008, 2142:23-2143:8 (emphasis added). This meant that "[t]hey were designed to fit together like puzzle pieces or . . . to work together without any signature programming on the part of the user." *Id.*

Another press release confirmed that MIMEsweeper came "with interfaces for virus protection packages such as . . . ThunderByte." JA14749-50. Dr. Spafford explained that this further confirmed that "the program [MIMEsweeper] was designed to work with those antivirus programs [ThunderByte 7.0] and clearly suggests that they be used together." JA8008, 2143:9-17. Accordingly, the evidence showed that ThunderByte 7.0 and MIMEsweeper were designed to work together and there was a "reasonable expectation of success" of combining the two products.

Finjan admits that these articles disclose that MIMEsweeper can be used with ThunderByte to scan email attachments but argues the articles do not establish that ThunderByte can be used with MIMEsweeper's gateway functionality. Br., 26-27. Finjan provided no evidence, however, that Dr. Spafford's testimony would not apply equally to scanning at the gateway. In fact, Dr. Spafford testified that *The MIMEsweeper Administrator Guide* taught that "the intended placement of

MIMEsweeper [was] at [the] gateway to serve as an e-mail gateway for virus scanning." JA8009, 2146:23-2147:6; JA14825.

Finjan's purported "unrebutted affirmative evidence that the [combination] was not possible" was the unsupported testimony of its own expert, Dr. Vigna. Br., 26-27. Dr. Vigna claimed that the combination was not possible based on his "experiments" with the prior art. *Id*. During cross-examination, however, Dr. Vigna admitted that he had not "seen" or even "been provided" with MIMEsweeper. JA8885, 3131:5-10. The jury thus was "free to credit (or discredit) [expert] testimony, and weigh it accordingly." *Rothman v. Target Corp.*, 556 F.3d 1310, 1319 (Fed. Cir. 2009).

(b) Defendants Presented Substantial Evidence That the Combination of ThunderByte with MIMEsweeper Discloses All Limitations of the Asserted Claims of the '194 Patent.

(i) Defendants Presented Substantial Evidence That ThunderByte Discloses the Use of "Security Profile Data" Including a "List of Suspicious Computer Operations."

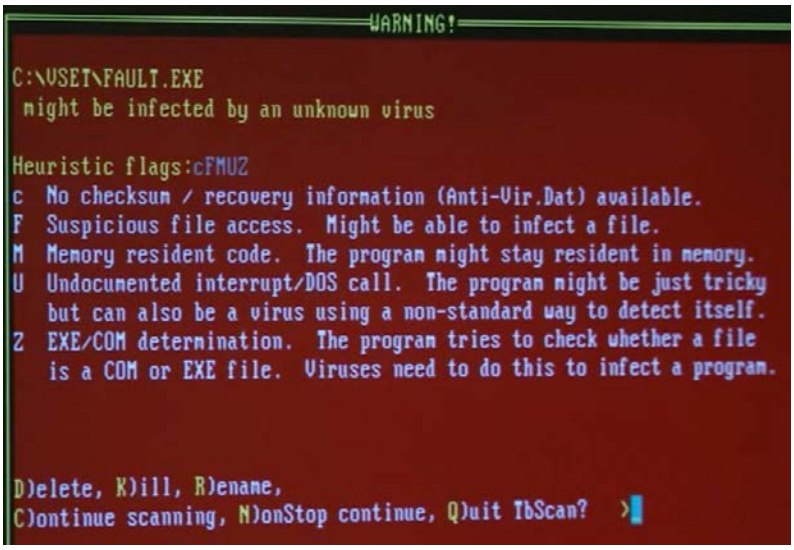
Citing specific portions of the *ThunderBYTE Anti-Virus Utilities User Manual* ("*User Manual*"), Dr. Spafford described in detail how ThunderByte identified a list of suspicious computer operations. For example, the *User Manual* stated: "TbScan will disassemble files. This makes it possible to detect suspicious instruction sequences and detect yet unknown viruses." JA15597; JA8009-10,

2149:6-2150:2. Based on this disclosure and others discussed below, Dr. Spafford concluded: "TbScan will look through the [D]ownloadable and find information to add the security profile that includes a list of suspicious computer operations that may be attempted by the [D]ownloadable." JA8009-10, 2149:16-2150:2.

The *User Manual* further explained that "if the purpose of those instructions appears to be formatting a disk or infecting a file, TbScan is going to issue a warning . . . [which] means [that ThunderByte is] able to detect suspicious operations as part of the [D]ownloadable." JA8010, 2150:3-17; JA15750 ("Every program contains instructions for the computer's microprocessor. By looking into the file's contents and interpreting the instructions, TbScan is able to detect the purpose of these instructions. If the purpose appears to be formatting a disk or infecting a file, TbScan issues a warning.").

The ThunderByte *User Manual* Appendix listed "flags" representing some of the "various kinds of suspicious operations that ThunderByte was able to recognize and would add to the [D]ownloadable profile." JA8010, 2150:18-2151:3; *see, e.g.*, JA15777 (listing flags, *e.g.*, F- Suspicious file access). Based on these disclosures, Dr. Spafford explained that ThunderByte detects when a program "access[es] a file in an unusual way" or "put[s] [itself] into the background so [it] would always be running to infect new files as users access [the new files]." JA8010, 2150:18-2151:9.

In addition, Dr. Spafford performed experiments using ThunderByte and showed the jury a screenshot (included in a demonstrative) from those experiments, which showed the list of the suspicious computer operations. JA8010-11, 2153:14-2154:7; JA29664. Dr. Spafford explained that the screenshot showed ThunderByte's output when he tried to "[r]un a program called fault.exe."



JA29664. Because fault.exe was a "virus that came out after the date on this version of ThunderByte," "it would have been unknown by ThunderByte." JA8010-11, 2153:19-2154:1. Dr. Spafford testified that the screenshot further showed that ThunderByte detected "F, Suspicious file access," which was just "one of the [five] suspicious operations that was detected by decompiling the fault.exe program." JA8011, 2154:2-7.

Finjan incorrectly argues that "it is only files' characteristics that are analyzed, not the actual operations of the files, as claimed." Br., 29. The '194

patent requires only "a list of suspicious computer operations that *may* be attempted." JA287, claim 1[b] (emphasis added). Because the "flags" set by ThunderByte represent "various kinds of suspicious operations that ThunderByte was able to recognize," JA8010, 2150:18-2151:3, ThunderByte detects suspicious computer operations that the Downloadable may attempt. For example, for fault.exe, ThunderByte detected "suspicious file access," which is a suspicious computer operation. JA8011, 2154:2-7.

Finjan also argues that the '194 patent teaches flagging "Downloadable[s] as malicious even if the sequence of bytes does not match a preexisting database." Br., 29. However, even though the term "a list of suspicious computer operations that may be attempted by the Downloadable" was raised at claim construction, Finjan never argued that the term required the detection of bytes that did not match a preexisting database. Instead, Finjan argued simply that the term should be given its plain and ordinary meaning. Finjan therefore waived this belated claim-construction argument by not raising it below. In any case, Dr. Spafford explained that ThunderByte can detect "unknown viruses," meaning that it can detect a malicious file "even if the sequence of bytes does not match a preexisting database." JA8009-10, 2149:16-2150:2; JA15597; Br., 29. Accordingly, the jury had more than substantial evidence that ThunderByte discloses the use of "security profile data" including a "list of suspicious computer operations."

(ii) Defendants Presented Substantial Evidence That It Would Have Been Obvious To Use a ThunderByte/MIMEsweeper Combination To Process JavaScript or Visual Basic Script.

Lastly, Defendants presented substantial evidence on which the jury relied to find that dependent claims 35 and 36, which require that "the Downloadable includes a JavaScript/Visual Basic script," were obvious. JA288, Claims 35, 36.

Finjan also attempts to challenge the invalidity of dependent claims 10, 11, and 33, which also require "wherein the Downloadables includes a Java applet/JavaScript/Visual Basic script." JA287, 288, Claims 10, 11, 33. These claims were not raised or even asserted at trial (JA7-8) and are thus waived. *See Wordtech Sys., Inc. v. Integrated Networks Solutions, Inc.*, 609 F.3d 1308, 1318 (Fed. Cir. 2010). In any case, the analysis as to claims 35 and 36 applies equally to these claims.

JavaScript and Visual Basic were developed by others and known at the time of the alleged invention. JA8012, 2159:5-2160:4. The Description of the Background Art of the '194 patent explained that "[e]xamples of Downloadables include . . . JavaScript scripts also developed by Sun Microsystems, Inc. . . . and Visual Basic also developed by the Microsoft Corporation." JA283, 1:49-55. Dr. Vigna also acknowledged that "in the mid '90s, all these technologies were introduced to add execution to web page." JA6970, 430:2-4.

The ThunderByte *User Manual* "made it clear that TbScan could scan items in other languages, such as JavaScript and Visual basic." JA8012, 2160:5-23 (referring to JA15652). The *User Manual* explained that the user can "fill out the extensions [they] want Tb to scan." *Id.* (referring to JA15652). Based on this, Dr. Spafford testified that it would have been obvious "as a matter of thinking of defense in depth to expand the scanning as necessary for any other kind of executable, [D]ownloadable executable," including JavaScript and Visual Basic files. JA8012-13, 2161:8-2162:3.

Defense-in-depth, discussed in Dr. Spafford's 1989 book, is the idea that "you put layers of defense in place against something bad that may happen . . . because if one layer failed in some fashion, or you forgot to turn it on, other layers would still be there to protect you." JA7995, 2091:9-2092:6. Applying the concept of defense-in-depth, a person of ordinary skill in the art would know that the ability to "fill out the extensions you want TbScan to scan" "allows [a user] to extend the scanning of a combination of MIMEsweeper and ThunderByte" to JavaScript and Visual Basic scripts. JA8012, 2160:12-19, 2161:8-19; JA15652. In fact, during the 1996 time frame, Dr. Spafford had personally expressed concerns about JavaScript or Visual Basic script files attached to e-mails containing viruses to the developers of the MIME standard used in MIMEsweeper. JA8012, 2160:20-2161:7.

In contrast, Dr. Vigna merely stated without any further basis that he had not "seen any evidence that the combination of these two references would be able to address [D]ownloadables that have JavaScript or Visual Basic Script." JA8869, 3069:12-21. Dr. Vigna never even responded to Dr. Spafford's application of the "defense-in-depth" concept. Accordingly, the district court correctly ruled that substantial evidence supported the jury's invalidity verdict. JA31.

2. Substantial Evidence Supports the Jury's Invalidity Verdict Based on SWEEP-InterCheck.

Sophos proved invalidity of the '194 patent by clear and convincing evidence based on its SWEEP-InterCheck product, which it developed and sold years before Finjan filed for its patents. Sophos's own employees provided unrebutted evidence about what SWEEP-InterCheck was and how it operated. Sophos founder Jan Hruska described in detail SWEEP's capabilities to detect unknown viruses, including polymorphic viruses. JA8095, 2325:3-2331:2. Tim Twaits, the engineer who created the first version of InterCheck, described how SWEEP and InterCheck worked together as a single product that denied access to infected files or programs by using a set of identities to prevent the execution of malicious code. JA8110, 2382:19-20; JA8110-11, 2383:10-2389:22; JA8113-14, 2396:11-2400:2. Mr. Klausner, Sophos's technical expert, was the only expert who reviewed the SWEEP-InterCheck source code. With this first-hand knowledge, he demonstrated how SWEEP-InterCheck practiced every element of

the asserted claims. JA8117-30, 2413:1-2463:5; JA 8175-78, 2466:17-2476:6. He also performed a live demonstration of SWEEP-InterCheck practicing the asserted claims of both asserted patents. JA8119-21, 2420:12-2426:14.

(a) Sophos Did Not Argue Anticipation Based on "Multiple Versions of Source Code."

Finjan wrongly argues that Sophos's proof of anticipation was "a combination of various Sweep [sic]-InterCheck source code and software versions and manuals . . . ." Br., 34. As the district court correctly found, Sophos relied on a single prior art reference—the SWEEP-InterCheck product demonstrated at trial—to prove anticipation. JA8110-11, 2384:19-2388:25; JA8119-21, 2420:12-2426:15; JA8126, 2446:6-2448:22. Mr. Klausner relied on SWEEP version 2.72 and InterCheck version 2.11 for his invalidity analysis. JA8181, 2488:8-11. He also referred to earlier versions of InterCheck (versions 2.01 and 2.10), and the evidence of record was that the functionality of these earlier versions was incorporated into version 2.11. JA8117-30, 2413:1-2463:5 (particularly JA8128, 2455:23-2456:9); JA 8175-78, 2466:17-2476:6. Further, all of Sophos's citations to source code were to SWEEP version 2.72 and InterCheck version 2.11, which were sold together as a single software product. JA8119, 2419:2-11; JA8122, 2431:24-2432:7; JA8123, 2435:4-19. Mr. Klausner confirmed that he performed no obviousness analysis because the software was sold as a single product.

JA8181, 2491:11-24. There was no evidence to the contrary, and Finjan cites no such evidence in its brief.

Finjan's reference to the "separate materials" in Sophos's demonstrative exhibit (Br., 35) is simply additional evidence, such as user manuals and VDL source code, that supports how SWEEP-InterCheck functioned at the relevant time. JA8099, 2340:3-17; JA8103, 2354:15-2355:12; JA8102, 2351:9-12; JA19490-501; JA19145-226. The user manuals and source code are not independent prior art references, but rather proof of how the SWEEP-InterCheck product operated. *Id.*; *see also* JA8110, 2383:4-9; JA8118, 2415:2-2416:5. The combination of a product with a contemporaneous manual that ships with the device is a single reference for anticipation purposes. *Enzo Biochem, Inc. v. Gen-Probe, Inc.*, 424 F.3d 1276, 1285 (Fed. Cir. 2005) (using product and "accompanying instructions" in anticipation analysis).

Finjan's argument is so lacking in merit that, during Finjan's closing statement to the jury, the district court was forced to give a curative instruction. Finjan argued that Sophos had relied on "several references and several pieces of source code and a lot of different source code." JA8997, 3412:24-25. Finjan then suggested it was improper to rely on source code because "[s]ource code is not public information." JA8997, 3413:16. The district court interrupted Finjan's closing statement, stating at sidebar that "it is very disingenous of you to argue to

this jury that source code is not publicly available. We all know that. These defendants have clearly relied on these products." JA8998, 3414:12-15. The court then gave a curative instruction to the jury:

> The defendants in this case relied on products as prior art, the products as prior art. They relied on source code, and the witnesses, the experts talked about source code, to demonstrate how the prior art products work and therefore demonstrate the invalidity, in their view, of the particular Finjan patents that are at issue.

JA08998, 3415:19-24. The court's instruction is a correct statement of the law and of the proof Sophos offered in support of its invalidity case, which the jury was entitled to accept.

(b) The Jury's Finding That SWEEP-InterCheck Discloses a Server That Serves as a Gateway to the Client Was Supported by Substantial Evidence.

Next, Finjan wrongly argues that SWEEP-InterCheck did not employ a "gateway." All of the evidence proves otherwise. Sophos employee Tim Twaits testified that the Downloadable cannot be downloaded to and executed by a client computer without first being scanned by SWEEP. JA8110-11, 2383:20-2387:23, JA8113-14, 2396:14-2400:2. This scan acts as the required gateway. And Sophos founder Dr. Hruska confirmed that the Downloadable is not executable on a computer before being checked by the SWEEP server: "Q: So it was already downloaded onto one of the computers before it hit the Sweep server. Is that correct? A: No, it's not correct." JA8107, 2372:14-16. As he confirmed,

SWEEP-InterCheck would "make sure that you can't do anything with [the Downloadable] before it's been checked." JA8114, 2399:7-2400:3. This testimony establishes that SWEEP-InterCheck acted as a gateway to prevent the execution of Downloadables.

Finjan ignores this testimony, citing only its expert's testimony. Br., 36-37 (citing JA8890-8891). Finjan's quotation of its expert's testimony stops right before he was impeached by the testimony of Sophos founder Hruska:

> Q. Let me show you Dr. Hruska's testimony on this point, at trial testimony 2378, 9 through 17, SOP DX-14-6.
>
> MR. ANDRE: Objection, Your Honor.
>
> THE COURT: Overruled.
>
> MR. ANDRE: Thank you, Your Honor.
>
> BY MR. ALLCOCK:
>
> Q. "Question: Can the file be accessed without being checked?
>
> "No."

JA8890, 3154:7-15. The jury was entitled to believe Dr. Hruska's testimony—along with all of the other evidence establishing that SWEEP-InterCheck acted as a gateway—over the self-serving and impeached testimony of Finjan's expert.

For the first time on appeal, Finjan also tries to cast this dispute as a claim-construction issue. Finjan never asked the district court to construe the claim term "gateway" or "serves as a gateway to the client." The district court construed only

three terms from the '194 patent: "Downloadable," "Downloadable security profile data pertaining to the Downloadable," and "a list of suspicious computer operations that may be attempted by the Downloadable." JA1834-37. Because Finjan never requested or obtained a construction of "gateway," it has waived any such claim-construction arguments on appeal. *Regents of Univ. of Minn. v. AGA Med. Corp.*, 717 F.3d 929, 946 (Fed Cir. 2013) ("*Regents*") (holding waiver of claim-construction arguments where party failed to raise construction in district court). Further, "gateway" appears only in the claims of the '194 patent, not in the specification, so Finjan's belated attempt to define that term by importing portions of the specification into the claims (Br., 38) fails.

(c) The Jury's Finding That SWEEP-InterCheck Discloses a Security Policy Was Supported by Substantial Evidence.

Sophos's expert methodically established that SWEEP-InterCheck discloses the use of a security policy. Sophos demonstrated how SWEEP-InterCheck could detect unknown malware, such as polymorphic viruses. JA8101-02, 2349:5-2351:5; JA8128, 2456:14-24. In fact, its security policy was used to determine whether malware, including polymorphic viruses, was present. JA8123, 2434:25-2435:19. Therefore, SWEEP-InterCheck used a security policy.

Finjan once again attempts to fabricate a claim-construction dispute, arguing that the asserted claims, "when properly construed, require a comparison of behavior to a policy, not just matching code against a known list of malicious code

. . . ." Br., 40. Finjan never raised this purported claim-construction dispute in the district court, so Finjan has waived it. *See Regents*, 717 F.3d at 946.

(d) The Jury's Finding That SWEEP-InterCheck Could Process JavaScript and Visual Basic Script Downloadables Was Supported by Substantial Evidence.

Sophos also proved, with unrebutted testimony and a demonstration, that SWEEP-InterCheck could process JavaScript and Visual Basic Downloadables. JA8120-21, 2425:25-2426:9; JA8125, 2443:11-2444:15. Even so, Finjan claims that SWEEP-InterCheck never possessed this capability. But as Mr. Klausner testified, the claims do not require that the Downloadable based on JavaScript or Visual Basic script actually contain the malware. JA8177, 2473:3-17. Rather, claims 35 and 36 simply recite "the Downloadable includes…" a JavaScript script or Visual Basic script. JA288 (emphasis added). During his demonstration for the jury—and without any objection from Finjan—Mr. Klausner demonstrated the SWEEP-InterCheck product as it processed Downloadables containing both JavaScript and Visual Basic scripts. JA8120-21, 2423:25-2424:7; 2425:25-2426:9.

Once again, Finjan tries to frame its quibbling with the evidence as a claim-construction dispute, arguing that the "District Court accepted Defendants' incorrect claim-construction argument that the claims do not require that the JavaScript or Visual Basic script be checked for malware." Br., 42. Defendants made no such argument. And Finjan never requested any construction of these

dependent claims, so it has waived any claim-construction challenge on appeal. *Regents*, 717 F.3d at 946. In arguing that the '194 patent "makes clear that JavaScript and similar type code are included in the security scan" (Br., 42), Finjan cites a portion of the specification that uses the suggestive words "may" and "preferably"—certainly nothing that would alter the plain meaning of "includes" in the dependent claims. Thus, the jury was entitled to rely on Sophos's substantial evidence that SWEEP-InterCheck practices the elements of claims 35 and 36.

(e) The Jury Was Not Limited to Considering SWEEP-InterCheck for Anticipation Only.

Contrary to Finjan's view, the jury was not limited to considering SWEEP-InterCheck for anticipation. "[A]nticipation is the ultimate of obviousness." *In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991). The Final Jury Instruction, which Finjan originally proposed, confirmed that "if [the jury] previously found something qualified as 'prior art' for anticipation purposes, it is likewise prior art for the obviousness determination." JA5277; JA172. Thus, the jury reasonably found the asserted claims obvious in light of SWEEP-InterCheck and the other prior art.

The trial record amply supports this finding. "Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved." *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17

(1966). Using these factors, Dr. Spafford explained to the jury the level of ordinary skill in the art at the time of the invention. JA7994-95, 2089:23-2091:3. Dr. Spafford explained that the concepts of defense-in-depth, static analysis, and dynamic analysis were all well-known in the prior art when the asserted patents were filed. JA7995-96, 2091:4-2096:21. Moreover, Dr. Spafford and Mr. Klausner, testified that there were no differences between the prior art and the claims at issue. *See supra*. Accordingly, substantial evidence supported a finding of either anticipation or obviousness for each reference.

For example, the jury was presented with a press release regarding MIMEsweeper stating that "MIMEsweeper has built-in interfaces for the majority of virus protection packages, including ThunderBYTE . . . and Sophos." JA14831. Thus, the jury had specific evidence regarding combining MIMEsweeper and Sophos's product. Having failed to argue why the asserted '194 patent claims were not obvious in light of SWEEP-InterCheck combined with the other prior art at trial (including MIMEsweeper), Finjan has waived this point. *See Cordance Corp. v. Amazon.com, Inc.*, 658 F.3d 1330, 1339 (Fed. Cir. 2011). This is yet another independent ground on which the invalidity verdict should be upheld. *See id.* (verdict "should be upheld if there was sufficient evidence to support any of the alternative theories of invalidity").

B. Defendants Presented Substantial Evidence That the '962 Patent Is Invalid.

Defendants also presented substantial evidence that the asserted claims of the '962 patent were invalid in light of SWEEP-InterCheck, NAV95, and HotJava.

1. Substantial Evidence Showed That the Asserted Claims of the '962 Patent Were Invalid In Light of SWEEP-InterCheck.

There was more than sufficient evidence to support the jury's finding that the asserted claims of the '962 patent were anticipated by SWEEP-InterCheck. Defendants presented substantial evidence demonstrating that SWEEP-InterCheck invalidated the asserted claims of the '962 patent. This evidence included testimony from Sophos's founder (Dr. Hruska), Sophos's employee who wrote most of the source code for SWEEP-InterCheck (Mr. Twaits), and Sophos's expert (Mr. Klausner). After presenting its case, Sophos demonstrated that "the evidence, taken as a whole, was sufficient to support the jury's verdict." *Northpoint Tech., Ltd. v. MDS Am., Inc.*, 413 F.3d 1301, 1311 (Fed. Cir. 2005).

(a) Sophos Proved That SWEEP-InterCheck Monitored Files "During Runtime."

Sophos presented credible evidence from multiple sources that established SWEEP-InterCheck's ability to monitor files "during runtime." Dr. Hruska testified in detail about SWEEP-InterCheck's functionality. JA8098, 2334:15-2336:8; JA8101-02, 2349:21-2351:5. And Dr. Hruska specifically testified that SWEEP-InterCheck monitored files while programs were running. JA8098,

2335:7-16. Furthermore, Mr. Twaits testified that SWEEP-InterCheck continued to monitor files while the programs were running. JA8114, 2399:7-18. Finally, Mr. Klausner offered his expert opinion that SWEEP-InterCheck monitors files "during runtime" (JA8127-28, 2453:3-2454:18) and ran a live demonstration of SWEEP-InterCheck doing just that. JA8120, 2425:12-24. Finjan ignores this evidence and neglects to mention that its own expert testified that SWEEP-InterCheck "actually monitored while the program is running. So it is actually performed at runtime." JA8876, 3095:10-11.

Finjan further confuses the issue by arguing that SWEEP-InterCheck merely provided a pre-runtime and post-runtime check. Br., 45. But this argument disregards Sophos's evidence demonstrating SWEEP-InterCheck's runtime monitoring functionalities. JA8098, 2334:15-2336:8; JA8101-02, 2349:21-2351:5; JA8112, 2391:20-2392:16; JA8127-28, 2453:3-2454:18. SWEEP-InterCheck's ability to provide pre- and post-runtime checks in addition to runtime checks does not preclude it from also monitoring files during runtime. Thus, SWEEP-InterCheck monitored files "during runtime."

(b) Sophos Proved That SWEEP-InterCheck Compared Information "Pertaining to the Downloadable Against a Predetermined Security Policy."

As with the "during runtime" element, Finjan discounts the extensive evidence demonstrating that SWEEP-InterCheck anticipated the '962 patent's

"pertaining to the Downloadable" limitations. Dr. Hruska and Mr. Twaits both testified that SWEEP-InterCheck used, in part, Sophos's proprietary Virus Description Language ("VDL") to compare information pertaining to the Downloadable against a predetermined security policy. JA8100-01, 2342:15-2346:1; JA8112, 2391:20-2392:16; JA8114, 2398:10-2399:1. Mr. Klausner then methodically explained how SWEEP-InterCheck compared information pertaining to the Downloadable against a predetermined security policy. JA8128-29, 2456:14-2458:3. This evidence strongly supports the jury's finding of anticipation. *Cordance Corp.*, 658 F.3d at 1339; *see also Northpoint Tech.*, 413 F.3d at 1311-12.

Unable to overturn the jury's invalidity verdict based on insufficient evidence, Finjan again resorts to belated claim-construction arguments to read non-existent limitations into the claims. Finjan now attempts to add the requirement that the "'962 Patent requires not only looking at the file being opened, but also looking at the file that made the original request to open the file." Br., 46. However, this requirement does not exist in any of the '962 patent's claims. And during claim-construction briefing, Finjan never mentioned this distinction. *See* JA811-12. Finjan cannot manufacture new constructions on appeal and has instead waived these arguments. *Regents*, 717 F.3d at 946. Finjan's belated claim

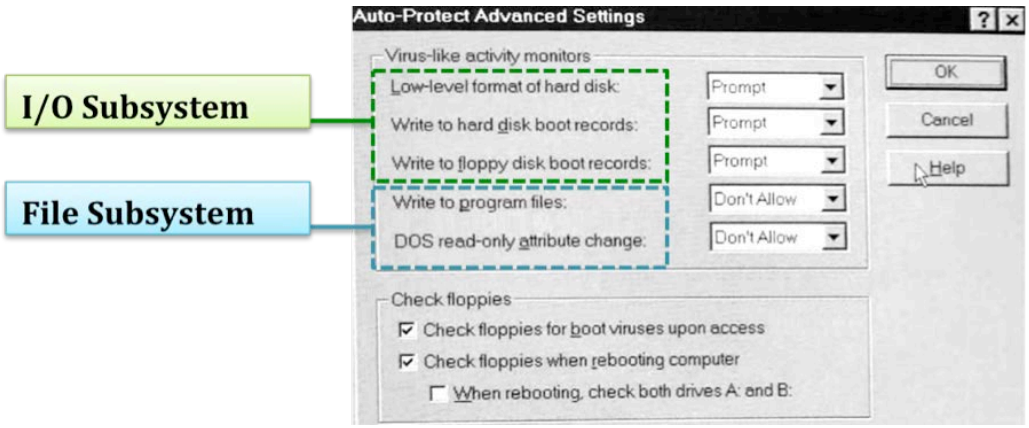
construction arguments do not overcome the substantial evidence supporting the jury's invalidity findings.

2. Defendants Presented Substantial Evidence That NAV95 and HotJava Invalidated the '962 Patent.

Defendants also presented sufficient evidence to support the jury's finding that the asserted claims of the '962 patent (besides claim 21) were invalid for additional independent reasons. Dr. Spafford presented substantial evidence that NAV95 disclosed all elements of claims 1, 5, 6, 12, 15, 33, 37, 38, 45, and 55. Additionally, Defendants presented substantial evidence that a combination of NAV95 and HotJava invalidated claim 52.

(a) Defendants Presented Substantial Evidence that NAV95 Monitored a "Plurality of Subsystems."

Finjan wrongly argues that it is entitled to JMOL because NAV95 did not monitor a plurality of subsystems. Br., 47. As the district court observed, "Dr. Spafford testified that NAV95 monitored the file subsystem and the I/O subsystem of the operating system." JA36. Dr. Spafford first explained that a "[s]ubsystem is a collection of data and routines that provide a set of collected functions that the computer performs through the operating system." JA7997, 2099:2-15. To demonstrate that NAV95 monitored a plurality of subsystems, Dr. Spafford next showed the jury a screenshot from using the NAV95 program and an excerpt from the *NAV95 User Manual*. JA17272; JA7997, 2099:16-2100:1; JA29629.



JA29629. The screenshot and *NAV95 User Manual* showed that NAV95 was able to monitor for certain virus-like activities. *Id.* Dr. Spafford explained that the I/O subsystem, or the "input-output subsystem," was the subsystem for "[r]eading and writing to disks but also to terminals, to printers, to other kinds of devices." JA7997, 2100:7-13. Since a program would have "to issue a very low level command as an output command to the disk itself to format it," detecting that would require monitoring the I/O subsystem. JA7997, 2100:14-19. Similarly, Dr. Spafford testified that monitoring writes to the boot records required monitoring the I/O subsystem since the boot records are hidden. JA7997-98, 2100:20-2102:2.

On the other hand, NAV95 would need to monitor the file subsystem for the last two activities: write to program files and DOS read-only attribute changes. The "[f]ile subsystem is a system that deals with those elements that have names, they are in directories, you can share those names, you can put them into programs, like editors. They have issues like date and time modified associated with those

files." JA7997, 2101:3-16. Moreover, because these two activities would be writing to or changing named files, those would relate to the file subsystem. *Id.*

Dr. Spafford then explained to the jury that the I/O subsystem and the file subsystem were two different subsystems. The I/O subsystem included "operations that have nothing to do with files, like reading and writing to the printer or the terminal." JA7997-98, 2101:17-2102:2. The "file subsystem has a whole set of activities that are separate from the I/O subsystem for named entities or directories." *Id.* The NAV95 source code—which Dr. Vigna could not review because he refused to sign the Protective Order—included two event handlers, one for each subsystem: Symantec I/O System Event Handler and Symantec File System Event Manager. JA29602-03; *see also* JA7998, 2102:3-2104:8; JA29630.

Finjan ignores Dr. Spafford's testimony in asserting that it provided "unrebutted testimony" from Dr. Vigna that the "'input/output' monitoring of NAV95 . . . are operations of the *file system*—not a distinct subsystem of the operating system." Br., 48. Not only is this conclusion contrary to Dr. Spafford's testimony, but it contradicts Microsoft's book on Windows 95, which specifically refers to the input/output subsystem as the "block I/O subsystem." JA16971.

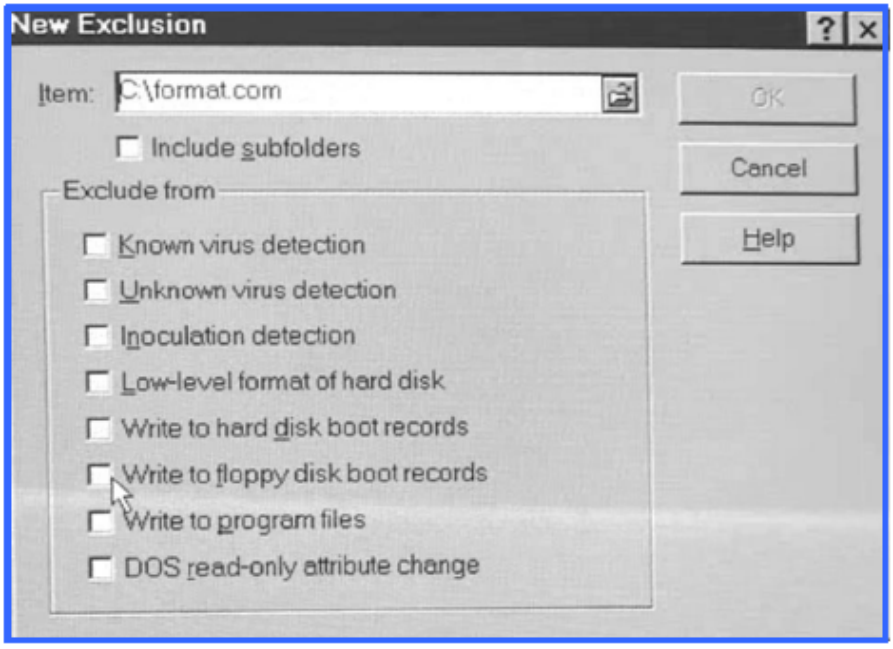
Dr. Vigna's own lecture notes also refute his trial testimony. JA17091. There, in the third bullet point, Dr. Vigna recognizes an I/O system separate and apart from the file system. Even when trying to explain his lecture notes, Dr.

Vigna acknowledges that these two different systems "work together to provide a *different level* of access for the devices." JA8883-84, 3126:12-3127:1 (emphasis added). Thus, the jury was free to credit the evidence that the I/O subsystem and the file system are distinct subsystems of the operating system and discredit Dr. Vigna's testimony to the contrary.

Finjan next argues that the I/O subsystem was not one of the four subsystems identified by the '962 patent and is not a subsystem "as a matter of claim construction." Br., 49. But, once again, "litigants waive their right to present new claim construction disputes if they are raised for the first time after trial." *Lazare Kaplan Int'l, Inc. v. Photoscribe Techs.*, Inc., 628 F.3d 1359, 1376 (Fed. Cir. 2010). Moreover, Finjan's technical infringement expert Dr. Medvidovic testified that Symantec infringed the '962 patent, in part, because Symantec products allegedly monitored the "registry subsystem" (which also is not listed in the '962 patent). JA7201, 741:18- 745:3. Finjan cannot now argue that the claims are restricted to the four types of subsystems disclosed in the specification. *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003) ("It is axiomatic that claims are construed the same way for both invalidity and infringement."). Substantial evidence thus showed that NAV95 monitored a plurality of subsystems.

(b) Defendants Presented Substantial Evidence That NAV95 Compared "Information Pertaining to a Downloadable Against a Predetermined Security Policy" and Performed a "Predetermined Responsive Action Based on the Comparison."

Defendants presented substantial evidence that NAV95 compared "information pertaining to a Downloadable." Dr. Spafford explained that NAV95 examined two types of information pertaining to a Downloadable: (i) the request made by a Downloadable (JA8000, 2110:15-2111:11), and (ii) the identity of the program making the request against an exclusion list (JA8000-01, 2111:12-2112:18, 2116:22-2117:5). Specifically, NAV95 would compare requests like whether a "downloadable is trying to format a hard disk" or "write to a floppy disk" against a security policy. JA8000, 2110:15-2111:11. Additionally, a user could modify the policy rules so that "files or whole directories" could be excluded. JA8000, 2111:16-23. This is not simply "excluding certain directories or files from being scanned" as Finjan argues. Br., 51. Dr. Spafford then showed the jury a screenshot of NAV95 demonstrating that NAV95 could exclude certain files from certain types of detection.



JA29639. Accordingly, Dr. Spafford presented two different methods demonstrating that NAV95 compared information pertaining to a Downloadable against a security policy.

Finjan argues that neither "action satisfies the requirement of comparing information about the Downloadable in question."[1] Br., 50. This position contradicts the position Finjan took during claim construction. Defendants contended that the term should be construed as "information that is sufficient to identify the requesting Downloadable." JA811-12. Finjan contended that the term should be given its plain and ordinary meaning and that Defendants' construction

[1] Finjan's brief further cites to the testimony of Ms. Frederiksen-Cross, Websense's expert, to interpret the term "information pertaining to a Downloadable." Br., 50. Ms. Frederiksen-Cross, however, was not testifying regarding the '962 patent because Websense was not accused of infringing the '962 patent. *See* JA8325, 2910:21-2911:4 (discussing the '194 patent).

"would unjustifiably narrow the term's broad scope." *Id.* Thus, Finjan's position at claim construction was that the term "information pertaining to a Downloadable" would include "information that is sufficient to identify the requesting Downloadable." The district court agreed with Finjan that the term should be given its plain and ordinary meaning. JA1836.

The claim language further contradicts Finjan's view. Dependent claim 53 requires: "comparing information pertaining to the Downloadable against a predetermined security policy, wherein information pertaining to the Downloadable *includes* information about *requests* to the operating system made by the Downloadable." JA310, claim 53 (emphasis added). Dr. Medvidovic, Finjan's technical infringement expert, also agreed that information pertaining to the Downloadable "could include . . . the request." JA7301, 1002:3-21. When asked on cross-examination, Dr. Vigna was unable to explain the discrepancy between his testimony and Dr. Medvidovic's interpretation of the claim term. JA8880, 3111:12-3113:7. Therefore, applying Dr. Spafford and Dr. Medvidovic's testimony regarding the scope of the term, Defendants presented substantial evidence that NAV95 compared information pertaining to a Downloadable.

(c) Defendants Presented Substantial Evidence That a Person of Ordinary Skill in the Art Would Have Been Motivated to Combine NAV95 With HotJava.

Finjan next contends that a person of ordinary skill in the art would not have been motivated to combine NAV95 and HotJava. But Dr. Spafford testified that the well-known principle of defense-in-depth provided a motivation to combine these products. JA8006, 2135:23-2136:19. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). It would have been obvious to a person of ordinary skill in the art to combine HotJava with NAV95 as HotJava "is a browser" and "will protect [] against [] some kinds of applets." JA8006, 2135:4-22.

Finjan's only response was that Dr. Spafford's analysis was hindsight analysis, but neither Finjan nor Dr. Vigna presented any evidence discrediting the defense-in-depth concept. Dr. Spafford further testified that he had *personal experience* running HotJava and NAV95 together in the *mid-1990s*. JA8006, 2136:4-12. Accordingly, there was substantial evidence that a person of ordinary skill in the art would have been motivated to combine NAV95 and HotJava.

(d) Defendants Presented Substantial Evidence That NAV95 Disclosed a "Downloadables Database."

Defendants also presented substantial evidence that claim 55 of the '962 patent was invalid. Finjan contends that NAV95 did not have a Downloadables

database because a "simple text activity log file" is not a database. Dr. Spafford presented substantial evidence that "[t]here is an explicit log file that is used for reporting information about the suspicious Downloadable, and what is done into a simple database, which is a log file." JA8002, 2118:14-21; JA17251-52. Finjan now attempts to argue that as a matter of claim construction, an activity log file cannot be a database. Finjan, however, has waived its right to raise the claim construction of "database" on appeal by failing to raise it during claim construction. *Lazare Kaplan*, 628 F.3d at 1376. Finjan also improperly seeks to introduce new evidence of how "database" should be construed. This evidence was not presented below. *Phonometrics, Inc. v. Westin Hotel Co.*, 319 F.3d 1328, 1333 (Fed. Cir. 2003) ("We, as a court of review, generally do not consider evidence that has not been considered by the district court.").

In any case, Dr. Spafford explained that a log file is a "database that is a sequential record of things that you want to record for looking up later, analyzing, doing other work with." JA8002, 2118:22-25. On cross examination, he further explained that an activity log "is a very simple form of database," "a flat-file database." JA8014, 2169:19-22. Substantial evidence thus supports the conclusion that an activity log file is a database.

3. Defendants Presented an Obviousness Argument for the Asserted Claims of the ’962 Patent.

Finjan incorrectly argues that, other than for claim 52 of the ’962 patent, Defendants relied only on anticipation to invalidate the asserted claims of the ’962 patent. Br. at 54. Dr. Spafford testified that the ’962 patent was invalid. JA7993, 2083:20-2084:1. As explained above, Dr. Spafford described how the prior art disclosed each element of the asserted claims. Dr. Spafford also laid out the *Graham* factors, including detailed testimony regarding the level of ordinary skill in the art and the scope and content of the prior art. JA7994-96, 2089:23-2096:21. Based on this, a jury could find that the ’962 patent was obvious. *In re Hayes Microcomputer Prods., Inc.*, 982 F.2d 1527, 1539 (Fed. Cir. 1992) (“Obviousness is a legal determination that may be submitted to a jury with proper instruction.”). Indeed, an expert need not testify to the legal conclusion of obviousness. *High Point Design LLC v. Buyers Direct, Inc.*, 730 F.3d 1301, 1313 (Fed. Cir. 2013.) (“[A]n expert’s opinion on the legal conclusion of obviousness is neither necessary nor controlling.”) (citations omitted).

Additionally, as described above in Section II.A.2(e), at the conclusion of the trial, based on an instruction proposed by Finjan, the court instructed the jury that “if [the jury] previously found something qualified as ‘prior art’ for anticipation purposes, it is likewise prior art for the obviousness determination.”

JA172. The court thus properly instructed the jury, at Finjan's request, to consider all prior art that was relevant for anticipation for obviousness too.

Further, for the '962 patent, Dr. Spafford specifically testified that the '962 patent was obvious in light of NAV95 combined with HotJava. JA8006, 2134:24-2136:22. Although Dr. Spafford testified regarding this combination while discussing claim 52, nothing limits his testimony to claim 52. In fact, claim 52 is identical to claim 1 of the '962 patent with the exception of the additional limitation "wherein the plurality of subsystems includes a network system." *Compare* JA306, JA310, claim 1 and 52. Thus, to the extent that claim 52 is obvious in light of NAV95 and HotJava, so is claim 1. And for the same reasons that NAV95 would have anticipated the asserted claims of the '962 patent, a combination of NAV95 and HotJava would have made the asserted claims obvious. Finjan also offered no argument why a combination of NAV95 and HotJava would not have invalidated the asserted claims.

Having been properly instructed and presented with substantial evidence, the jury was also free to find that the asserted claims were obvious in light of a combination of other pieces of prior art, *e.g.*, a combination of NAV95 and SWEEP-InterCheck. Finjan fails even to address any obviousness argument for the '962 patent besides the combination of NAV95 and HotJava. Finjan thus has

failed to show that there was not "sufficient evidence to support any of the alternative theories of invalidity." *Cordance Corp.*, 658 F.3d at 1339.

C. The District Court Properly Exercised Its Discretion in Denying Finjan's Motion for a New Trial on Invalidity.

1. The District Court Properly Precluded Finjan's Expert From Providing Misleading Testimony About His Purported Review of Binary and Assembly Language Code.

The district court was well within its discretion to preclude Finjan's expert, Dr. Vigna, from testifying about his purported review of binary and assembly code for the prior art products. All the other experts in this case (including Finjan's other experts) relied on the source code of the relevant products—the admitted "DNA" of the products.

Throughout the case and trial, the parties focused on the source code of the prior art products as the best evidence of how the products operate. During its opening statement, Finjan explained that "[s]ource code, to computer scientists, that is the good stuff. That is the DNA of what is happening." JA6947, 339:16-18. Finjan's infringement expert testified that source code is the DNA of the systems in question. JA7197, 725:2-5 ("I relied on source code, which is kind of, as it was characterized earlier in the proceedings, the DNA of the system in question."). Defendants' experts also focused on the source code of the prior art products. JA7996, 2097:12-20; JA7998, 2102:3-2105:3; JA8004, 2128:22-2129:3; JA8004-05, 2129:16-2130:13.

Finjan had a problem of its own making because its validity expert, Dr. Vigna, founded and works for a competitor of Defendants. JA6976, 455:11-16; JA6977, 456:12-457:4; JA8851, 2996:21-2998:7; JA8852, 2999:14-23. Dr. Vigna therefore chose not to sign the protective order and could not review the source code for the prior art products. Without the ability to present meaningful testimony about the admitted DNA of the prior art products, Dr. Vigna instead attempted to mislead the jury by offering conclusory testimony during his direct examination that he allegedly reviewed the binary and assembly code for such products. JA8859-60, 3030:7-3031:4.

During his direct examination, Dr. Vigna did not provide any details about his alleged review of the binary and assembly code, nor did he testify that these materials were more meaningful than the source code. On cross-examination, Defendants demonstrated that Dr. Vigna did not review the source code for any of the prior art products. *Id.*, JA8888, 3143:3-6; JA8888, 3143:24-3144:10. On redirect, Finjan's counsel attempted to elicit testimony from Dr. Vigna that the binary code he reviewed for the SWEEP-InterCheck product was a better source of material than the actual source code. The district court was forced to intervene to prevent Dr. Vigna from confusing the jury:

> Q: Now, you mentioned binary code in connection with Sweep/InterCheck, and you thought this was a better source of material. Why is that?

> THE COURT: Let me see counsel.
>
> (The following discussion took place at sidebar.)
>
> THE COURT: It's not my job to judge this witness' credibility, but I am not going let him confuse this jury with a discussion about binary code. No expert in this case has talked about binary code, including this gentleman on his direct testimony. I have about had it with him. So I'd avoid that area if I were you.

JA8892, 3159:15-3160:1.

As the district court noted, the parties and all the other technical experts in the case addressed source code, not binary code. Under these circumstances, Dr. Vigna's redirect testimony without the benefit of any source code review would have been unreliable, prejudicial, and misleading under Federal Rules of Evidence 403 and 702. Indeed, during his direct examination, Dr. Vigna admitted it was "almost impossible to understand what's really going on" by reviewing binary code comprised of ones and zeros. JA8859, 3030:20-22. Finjan and Dr. Vigna also did not establish that reviewing binary code was a reliable method. *See Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1373-74 (Fed. Cir. 2013) (district court abused its discretion in admitting unreliable expert testimony). Thus, Finjan's problem was one of its own making, and it should not be given a new trial because the district court had to issue a corrective instruction resulting from Finjan's misleading argument.

At sidebar, Finjan's counsel did not submit an offer of proof for the testimony Dr. Vigna would have offered, nor did counsel explain the relevance of such testimony. And Finjan does not cite any legal or technical support for the position that binary code is more relevant than source code. During Finjan's rebuttal closing statement, the district court correctly issued a curative instruction when Finjan improperly suggested that the law does not allow the jury to consider the source code for the prior art products. *See Touchcom, Inc. v. Bereskin & Parr*, 790 F. Supp. 2d 435, 453-54 (E.D. Va. 2011) (rejecting argument that product was not prior art because the public would not be able to see its source code); *Zenith Elecs. Corp. v. PDI Commc'n Sys., Inc.*, 522 F.3d 1348, 1356 (Fed. Cir. 2008) ("[T]he public use itself need not be enabling.") (citation omitted). That is precisely where Finjan was going when it attempted to elicit the testimony from Dr. Vigna regarding the binary code. Indeed, when Defendants raised this as an evidentiary issue before trial, Finjan agreed that it "will not offer Dr. Vigna's limited testimony regarding the non-enablement" of the software products relied upon by Defendants. JA6145. The district court, therefore, was well within its discretion to preclude Dr. Vigna from testifying about binary code.

2. Finjan Failed to Prove that the Verdicts of Invalidity and No Infringement by Sophos Are Logically Inconsistent.

The district court did not abuse its discretion in denying a new invalidity trial based on Finjan's assertion that the verdicts were inconsistent. The bar for

disturbing a jury verdict as inconsistent is very high: "a court may order a new trial based on inconsistent verdicts only if 'no rational jury could have brought back the verdicts that were returned.'" *Monaco v. City of Camden*, 366 Fed. App'x 330, 331 (3d Cir. 2010) (quoting *Pearson v. Welborn*, 471 F.3d 732, 739 (7th Cir. 2006)). Moreover, a district court is first obligated "to 'attempt to reconcile the jury's findings' to determine 'whether the jury could have, consistent with its instructions, rendered the challenged verdicts.'" *Id.* (quoting *Davignon v. Hodgson*, 524 F.3d 91, 109 (1st Cir. 2008)). The court may "allow an apparently inconsistent verdict to stand" or "read the verdict in a manner that will resolve the inconsistencies." *Acumed LLC v. Advanced Surgical Servs., Inc.*, 561 F.3d 199, 217 (3d Cir. 2009); *see also Mosley v. Wilson*, 102 F.3d 85, 90-91 (3d Cir. 1996). Additionally, the verdict "should be upheld if there was sufficient evidence to support any of the alternative theories of invalidity." *Cordance Corp.*, 658 F.3d at 1339.

As an initial matter, Finjan waived any challenge to the alleged inconsistency in the verdict because it failed to object on this ground before the district court discharged the jury. *See Simmons v. City of Philadelphia*, 947 F.2d 1042, 1056-57 (3d Cir. 1991) ("In this circuit, it probably is necessary, as it is in the majority of the circuits, to raise prior to the jury's dismissal an objection based on the inconsistency of the answers to interrogatories supporting a general verdict

rendered under Rule 49(b).”). Finjan made no such objection here, and has thus waived any inconsistency challenge to the verdict. JA9389-90, 3431:7-3436:12. *See Function Media, LLC v. Google Inc.*, 708 F.3d 1310, 1327-30 (Fed. Cir. 2013) (holding that a verdict that asked simple yes/no questions regarding infringement, anticipation, and obviousness was a general verdict under Rule 49(b) and that, because the appellant did not object to the inconsistency in the verdict prior to discharge of the jury, it had waived that challenge on appeal).

Even if not waived, Finjan’s challenge based on alleged inconsistency fails because the verdicts of invalidity and no infringement by Sophos are easily reconciled on any and all of five independent grounds.

First, different parties bore the burdens of proof on invalidity and infringement. Defendants had the burden of proving invalidity, while Finjan had the burden of proving infringement. Contrary to Finjan’s suggestion, Sophos had no burden to prove noninfringement, nor even to come up with any evidence or argument negating infringement. *See, e.g., Medtronic, Inc. v. Mirowski Family Ventures, LLC,* 134 S. Ct. 843, 849 (2014); *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1534 n.4 (Fed. Cir. 1983). The jury was entitled to find that Finjan had failed to meet its burden of proving infringement while finding that Defendants met their burden of proving invalidity, irrespective of the relationship between Sophos’s accused products and the invalidating prior art.

Second, the jury was not obligated to accept Sophos's attorney's argument about whether Finjan's patents covered what Sophos does. Attorney argument is not evidence. *See, e.g.*, *Gemtron Corp. v. Saint-Gobain Corp.*, 572 F.3d 1371, 1380 (Fed. Cir. 2009); *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1581 (Fed. Cir. 1989). The jury thus could not treat the argument as evidence. The jury also was not obligated to agree with Sophos's counsel's argument but instead was entitled to disregard the argument and decide for itself whether Finjan had proven infringement. Additionally, the district court properly found that Sophos's counsel's argument about what the patents cover did not amount to unequivocal admissions of infringement by Sophos. JA62-63. As the court noted, Sophos included infringement as a disputed issue in both the pre-trial order and jury verdict form and questioned the credibility of Finjan's infringement expert. *Id.*; JA5.

Third, the trial record contains substantial evidence that Sophos did not infringe either the '962 or '194 patent. Finjan does not even contest this point on appeal and thus has waived it. *See Aventis Pharma S.A. v. Hospira, Inc.*, 675 F.3d 1324, 1332-33 (Fed. Cir. 2012). As the district court properly recognized, the trial record supported the conclusion that Finjan failed to prove that Sophos's products practiced the "monitoring" element of the '962 patent. JA59-61. The same is true

of the "comparing" element of the '194 patent. *Id.* These are additional reasons why there was no logical inconsistency in the jury's verdicts.

Fourth, the jury was free to disbelieve Finjan's expert's infringement testimony as not credible. For example, as discussed in greater detail in the preceding section, Sophos demonstrated that Finjan's expert had not considered Sophos's source code, failed to adequately determine the accused products' functionalities, and did not know what the acronym "VDL" stood for until trial began despite using VDL ("Virus Description Language") in his infringement analysis. It was entirely permissible for the jury to discredit his infringement-related testimony while finding that Sophos had met its burden of proving invalidity. *See Star Scientific, Inc. v. R.J. Reynolds Tobacco Co.*, 655 F.3d 1364, 1378 (Fed. Cir. 2011); *Motorola, Inc. v. Interdigital Technology Corp.*, 121 F.3d 1461, 1470-71 (Fed. Cir. 1997) (finding verdicts of noninfringement and invalidity were not inconsistent because expert testimony afforded sufficient basis for the jury's verdict).

Not only is Finjan's argument meritless, but it applies, at most, only to claim 21 of the '962 patent. This is because every other claim of each asserted patent had at least one completely non-Sophos-prior-art invalidity argument leveled against it at trial. As for all other asserted claims, a fifth reason why the verdicts are not inconsistent is that the jury may have based these invalidity verdicts on the

non-Sophos art. *See Cordance Corp.*, 658 F.3d at 1339. Further, Finjan's assertion that only Sophos art was argued for anticipation of the '194 patent (Br., 65) is irrelevant. This is because the jury also found the '194 patent obvious (JA7) and could have done so based on non-Sophos prior art or, as explained in Section II.A.2(e) above, on a combination of SWEEP-InterCheck with other art. And Finjan has cited no law requiring the verdict form to have included special interrogatories for each prior art reference and invalidity theory.

Without citing any legal authority, Finjan also asserts in passing that the jury verdict was ambiguous because the verdict form was not partitioned according to each prior art reference and combination. Br., 65. According to Finjan, this argument is relevant only if the verdicts were in fact inconsistent. *Id.* Because the verdicts are consistent for the reasons given above, Finjan's argument is irrelevant. Additionally, Finjan has waived this argument by failing to cite any legal authority to support it. *See Rimas Properties, LLC v. Amalgamated Bank*, 451 Fed. App'x 163, 164 n.3 (3d Cir. 2011) ("Because Rimas fails to provide legal authority in support of this argument, we deem the issue waived.") (citing *Kost v. Kozakiewicz*, 1 F.3d 176, 182 (3d Cir. 1993)). Finally, the district court has discretion to determine the content and structure of the jury verdict form. *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1248 (Fed. Cir. 2010). Especially in view of the use of similar forms in other multi-reference invalidity cases, Finjan failed to show that the

district court abused its discretion here. *See, e.g.*, *Cordance Corp.*, 658 F.3d at 1333; *i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 845 (Fed. Cir. 2010).

Finjan also complains in a footnote that the jury took two hours to decide invalidity after asking the district judge a question about the relationship between infringement and invalidity. Br., 65 n.6. Arguments made in a footnote are waived. *See SmithKline Beecham Corp. v. Apotex Corp.*, 439 F.3d 1312, 1320 (Fed. Cir. 2006). Moreover, Finjan cites no authority for its view that Finjan's speculation about the amount of time the jury took to reach its invalidity verdict has any bearing on the consistency or soundness of that verdict.

Finally, even if Finjan's inconsistency argument had any merit, it would be limited to the jury's verdict of anticipation and would have no effect on the jury's verdict that both asserted patents were invalid as obvious (JA7-8). *See Comaper Corp. v. Antec, Inc*., 596 F.3d 1343, 1349, 1354-55 (Fed. Cir. 2010) (upholding infringement verdict but finding obviousness verdict inconsistent, and remanding for a new trial only as to the obviousness verdict); *see also Motorola*, 121 F.3d at 1471 ("To the extent that this court finds substantial evidentiary support for the obviousness verdicts, it need not consider the question of whether the claims are also anticipated."). Even if an element of an asserted claim were found lacking in SWEEP-InterCheck, the jury still could have found the claim obvious in view of a

combination of SWEEP-InterCheck and other art for the reasons discussed in prior sections.

Finjan does not challenge the judgment of no infringement by Sophos on appeal, but rather seeks to parlay it into a new trial on invalidity. But its arguments lack both legal authority—Finjan hardly even tries to cite any—and factual substance. Accordingly, Finjan's request for a new trial on invalidity should be rejected.

3. The District Court Properly Exercised Its Discretion in Denying a New Trial Because the Invalidity Verdict Was Not Against the Great Weight of the Evidence.

Finjan's final plea for a new trial simply incorporates its JMOL arguments (Br., 66-67), which the Defendants have rebutted above. Finjan also wrongly suggests that it is *per se* easier to obtain a new trial on appeal than to overcome the denial of JMOL on appeal. *Id.* While the new trial standard is lower than the JMOL standard at the district court level, Finjan ignores the fact that this Court reviews the denial of a new trial motion for abuse of discretion rather than *de novo*. (*See* Standard of Review section, *supra*.) In all events, Finjan has failed to show it is entitled to either JMOL of validity or a new invalidity trial.

D. Finjan Has Waived Any Challenge to the Jury's Verdict That Defendants Did Not Infringe the Asserted Patents.

Finjan does not challenge the district court's finding that substantial evidence supported the jury's verdict that Defendants did not infringe either of the

asserted patents. Accordingly, Finjan has waived any challenge to that portion of the jury's verdict. *Advanced Magnetic Closures, Inc. v. Rome Fastener Corp.*, 607 F.3d 817, 833 (Fed. Cir. 2010) ("This court has consistently held that a party waives an argument not raised in its opening brief."); *Aventis Pharma S.A. v. Hospira, Inc*., 675 F.3d 1324, 1332-33 (Fed. Cir. 2012) (where appellant failed to address district court's obviousness finding in its opening brief, any challenge to that finding was waived). Thus, the jury's noninfringement verdict must stand.

CONCLUSION

The judgment should be affirmed in its entirety.

Dated: February 24, 2014

Respectfully submitted,

/s/ David A. Nelson
Jennifer A. Kash
Sean S. Pak
David A. Nelson
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111
Telephone: (415) 875-6600

Attorneys for Defendant-Appellee Symantec Corp.

/s/ Anthony M. Stiegler (with permission)
Anthony M. Stiegler
Lori R. Mason
COOLEY LLP
4401 Eastgate Mall
San Diego, California 92121
Telephone: (858) 550-6000

Attorneys for Defendant-Appellee Websense, Inc.

/s/ John Allcock (with permission)
John Allcock
Sean C. Cunningham
Stanley J. Panikowski
Kathryn Riley Grasso
DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, California 92101
Telephone: (619) 699-2700

Attorneys for Defendant-Appellee Sophos Inc.

United States Court of Appeals
for the Federal Circuit

Finjan Inc. v. Symantec Corp, 2013-1682

CERTIFICATE OF SERVICE

I, John C. Kruesi, Jr., being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

Counsel Press was retained by COOLEY LLP, attorneys for Appellee Websense, Inc. to print this document. I am an employee of Counsel Press.

On **February 24, 2014** counsel for Appellee has authorized me to electronically file the foregoing **Brief for Defendants-Appellees** with the Clerk of Court using the CM/ECF System, which will serve via e-mail notice of such filing to all counsel registered as CM/ECF users, including any of the following:

Paul J. Andre
(Principal Counsel)
Lisa Kobialka
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
650-752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com

Aaron M. Frankel
Kramer Levin Naftalis
& Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
212-715-7793
afrankel@kramerlevin.com

Jeffrey Matthew Harris
Bancroft PLLC
1919 M Street, N.W., Suite 470
Washington, DC 20036
202-640-6527
jharris@bancroftpllc.com

Paper copies will also be mailed to the above principal counsel at the time paper copies are sent to the Court.

Upon acceptance by the Court of the e-filed document, six paper copies will be filed with the Court, via Federal Express, within the time provided in the Court's rules.

February 24, 2014

/s/ John C. Kruesi, Jr.
John C. Kruesi, Jr.
Counsel Press

CERTIFICATE OF COMPLIANCE

The undersigned certifies that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B). This brief contains 13,777 words as calculated by the "Word Count" feature of Microsoft Word 2013, the word processing program used to create it.

The undersigned further certifies that this brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6). This brief has been prepared in a proportionally spaced typeface using Microsoft Word 2007 in Times New Roman, 14 point font.

Dated: February 24, 2014

/s/ David A. Nelson
David A. Nelson

Attorneys for Defendant-Appellee Symantec Corp.